Homework Assignment 3: Risk & Mitigation

Matthew Austin

Fontbonne University

Quagliata

18 October 2016

**Risk & Mitigation Policy**

***1. Purpose***

This Risk and Mitigation policy provides the movement for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis. The aim of risk management is to maximise opportunities in all of the organization's activities and to minimise adversity. Specifically, the Risk & Mitigation Policy is for controlling these risks (a situation involving exposure to danger) through a formal process which is necessary for the well-being of the organization and everyone in it. The jobs and services the organization provides, the safety of the workplace and other benefits all depend to an extent on our ability to control and mitigate (make less severe, serious, or painful) risks.

***2. Scope***

This policy defines the security policy for Risk & Mitigations within our organization to ensure protection of such data.

***3. Definitions***

**Encryption:** is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties.

**Certificate:** A digital representation of information: A set of data that uniquely identifies an entity, contains the entity’s public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its cryptoperiod.

**Data Monitoring:** is adata monitoring committee (DMC) – sometimes called a data and safety monitoring board (DSMB) – is an independent group of experts who monitor patient safety and treatment efficacy data while a clinical trial is ongoing.

**Data Classification:** Data classification is the process of organizing data into categories for its most effective and efficient use. A well-planned data classification system makes essential data easy to find and retrieve. This can be of particular importance for risk management, legal discovery, and compliance.

**Least Privilege:** The security objective of granting users only those accesses they need to perform their official duties.

***4. Policy***

The development, implementation, and execution of this Risk and Mitigation Policy (RMP) is the primary responsibility of the specific business unit for whom the RMP is being developed in cooperation with the Infosec Team. Business units are expected to properly facilitate the RMP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the in the development and maintenance of a Security Response Plan. (Sans)

*4.1 Classification*

* All information should be simple and easy to find by creating an effective data classification app with an algorithm that safely and effectively receives and sends data within the server.
* The classification software can either be created by software development team in the organization. If a software development team is not available, the use of a third party's system is acceptable (make sure that the software is trusted and secure).
  + Whether or not the software is created by a software development team or acquire via third party, the software should be regularly updated.
* With the classification software the user's role in the organization should correlate with their access to certain items in the server by following the rules of least privilege.

*4.3 Risk Assessment & Management*

* The organization's approach to security should be based on risk assessments.
* Every member of the organization must be knowledgeable of their role and know and control all the information that they have granted control over.
* The organization should continuously (24/7) scan and assess the risk and evaluate the need for protective measures. If cost is a concern for the organization, a scanning and assessment schedule shall be revised based on its budget (and SSAE 16 Report if accessible). Nonetheless scans and risk assessments should at least be done annually.
* The Chief Security Office (CSO) must overlook risk assessments which must identify, quantify and prioritize the risks according to relevant criteria for acceptable risks. When changes are made the risk assessment must be change/updated as well.
* The CSO must assess the and effective and suitable consequence to users who violate anything in the policy. To determine whether
* Risk assessments must be approved by the management of the organization and system owners
* If a risk assessment reveals unacceptable risks, measures must be implemented to reduce the risk to an acceptable level.

*4.1 Risk Mitigation*

4.1.1 Information Security

* + Ensure servers and high-priority documents are protected in password-protected rooms watched 24/7 by security officials and cameras that detect unauthorised movement/access in the room and notifies all security officials in the building. Based on the level data/information within the company the level of concern (LOC) should determine the level of security of that information through assessment.
  + Educate those to not share information with others, not even to fellow peers. If so direct them to a Data Monitoring Committee official if the password has been forgotten or their intentions seems suspicious.
  + Emails and user activity are monitored 24/7 by an assigned data monitoring committee officials along with a learning algorithm that inhibits certains actions and access of the user if a threat is foreseen.
  + Ensure that the server and every account in the server password is reset every 30 days.
  + Any user who request information that is out of their privilege must be directed to the CSO or Data Monitor Committee (DMC).

4.1.2 Natural Disaster

* + In the event that there is a power outage of a natural disaster that threatens the servers, the backup generator automatic power on to ensure that data is restored automatically while running a diagnostic and security test on all of the data in rest in the building to ensure that everything is running smoothly, secure and to assess any loss of data.\
* All users in the organization must collaborate with the operational users to create a understanding of the risks and their implications. Such risks can be classified as impacting traditional cost, schedule, and performance parameters.
* Provide users with projections of schedule adjustments needed to reduce risk associated with technology maturity or additional development to improve performance.
* Help control risks by performing analyses of various mitigation options (which are alternative plans/policies created by CSO and/or Data Monitoring Committee and/or software owner.
* Determining the needs of the the different roles/levels of the organization after assessing and revealing a risk/threat.
* Finally create a contingency plan (plan B) that should be created by the CSO and/or Data Monitoring Committee and/or software owner. Otherwise, assess and scan every back-up until it seems secure.

Reference

Campus Information Technology Security Policy. (2016). Retrieved August 22, 2016,

from <https://security.berkeley.edu/campus-information-technology-security-policy>

<https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en>

The University Policy Manual. (2016). Retrieved August 22, 2016, from

<https://policy.uncg.edu/university-policies/data/>

Secure The Breach | Get Ready For A Security Breach. (n.d.). Retrieved August 30,

2016, from <http://www.securethebreach.com/encryption.html>

Information Security | Washington University in St. Louis. (2016). Retrieved August 22,

2016, from <https://wustl.edu/about/compliance-policies/computers-in>

Risk Mitigation Planning | MITRE (2016). Retrieved October 9,

2016 from https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring